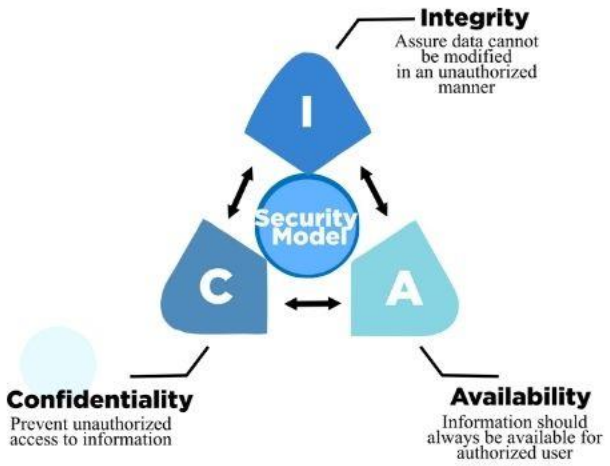
IoT Security: Solutions to Mitigate Attacks

FIU | FLORIDA INTERNATIONAL UNIVERSITY

Andrea Gisselle Menjivar || amenj003@fiu.edu || Master in IoT

I. Introduction

The Internet of Things (IoT) is transforming everyday life by connecting real-world devices to the cloud. However, this growing interconnectivity comes with an increased risk of cyberattacks. IoT devices, used in industries like healthcare, transportation, and smart cities, often lack robust security—leaving them vulnerable to a wide range of threats. 85% of organizations use IoT, but 90% lack confidence in its security. 70% of devices are vulnerable when online.



II. Methodology

This research reviews literature from 2019 to 2024 on mitigation strategies for IoT attacks. It categorizes common security methods tested, implemented, or proposed by other researchers to understand effective ways to secure IoT systems.

+85% of global organizations are projected to utilize IoT devices.
70% of IoT devices are vulnerable to at least one serious security flaw.
90% of businesses lack confidence in their IoT security.

III. Key Mitigation Techniques

Cyber Deception
Creating decoy IoT devices and fake network components to mislead attackers and collect forensic data. Techniques include honeypots, moving target defense, and deception frameworks.

REST APIs + Middleware
REST APIs protect communication between IoT devices and the cloud using middleware authentication. This approach helps prevent man-in-the-middle (MITM) attacks and unauthorized data access.

Blockchain Integration
Blockchain offers secure, decentralized recordkeeping for IoT data and firmware. Benefits include digital signatures, trusted updates, and access control without a central authority.

Machine Learning
ML algorithms such as decision trees and ensemble models detect botnets and anomalous traffic patterns. These techniques strengthen intrusion detection systems (IDS).

Fog Computing
A hybrid IDS framework using fog nodes reduces processing on resource-limited IoT devices. This model combines signature-based and anomaly-based detection methods.

VI. Threats & Countermeasures by Layer

IoT Layer	Threats	Countermeasures
Sensing	Hardware attacks, side-channels	Lightweight cryptography, digital signatures
Network	DoS, eavesdropping, routing attacks	Encrypted routing, secure key exchange
Middleware	Data interception, unauthorized acces	Blockchain, secure middleware
Application	User impersonation, data breaches	Multi-factor authentication, firewalls

V. Conclusions

IoT systems are exposed to diverse threats like botnets, DoS, and MITM attacks. This study presents current mitigation strategies using deception, blockchain, ML, fog computing, and more. While no system is completely secure, combining these solutions greatly enhances IoT reliability. Continuous research is essential to address evolving cyber threats.

unitec Investigación | ceutec | Revista de Ciencias Forenses de Honduras | Scientific.Net Publisher in Materials Science & Engineering | Emergent | INNOVARE Revista de ciencia y tecnología | Tekné Ciencias Sociales y Humanidades